



Securing Your Web World

Trend Micro™ Intrusion Defense Firewall Security Advisory

*Microsoft Windows MPEG2TuneRequest ActiveX
Control Object Vulnerability (Microsoft Security
Advisory - 972890)*

Version 1.0

7/7/2009



IDF Security Advisory

Intrusion Defense Firewall Security Research Team

The IDF Security Research team is comprised of security experts who monitor the latest threats and develop new security rules that protect against these threats. The team helps customers stay ahead of the threat curve by:

- **Monitoring & Research:** Over 100 sources of public, private and government data are systematically and continuously monitored to identify and correlate new relevant threats and vulnerabilities.
- **Microsoft Active Protections Program (MAPP) membership:** MAPP is a new program for security software providers which provides us with vulnerability information from the Microsoft Security Response Center in advance of Microsoft's monthly security update.
- **Creating Security Advisories:** Detailed descriptions of security vulnerabilities
- **Delivering Security Updates:** Security rules that shield vulnerabilities in operating systems and applications until patches can be applied. This reduces the window of exposure to attack, while enabling customers to patch their systems as per their standard process and avoid the need for costly, inefficient emergency patching.

Vulnerability: Microsoft Windows MPEG2TuneRequest ActiveX Control Object (MS Advisory 972890)

Executive Summary

A remote code execution vulnerability in a Microsoft Video ActiveX Control. An attacker who successfully exploits this vulnerability could gain control over the affected system with the same user rights as the local user.

This is a zero-day vulnerability as we are aware of attacks attempting to exploit this vulnerability and no patches are available from Microsoft to address this vulnerability.

Trend Micro™ released an emergency Security Update that contained three new security rules to shield this vulnerability from attack:

- **Rule 1003606:** Microsoft Windows 'MPEG2TuneRequest' Object Remote Code Execution
- **Rule 1003605:** Microsoft Windows 'MPEG2TuneRequest' Object Remote Code Execution Vulnerability

- **Rule 1003609:** Com Object Instantiation Memory Corruption – July 2009

In addition to these new rules, an existing IDF rule (*1002061: Identified Suspicious JavaScript Encoded Shellcode*) would have also protected against currently known exploits of this vulnerability.

Technical Details

The msvidctl.dll component of Microsoft DirectShow contains a stack overflow vulnerability in the way it processes DirectShow MPEG2TuneRequests. When using Internet Explorer, code execution is remote and may not require any user intervention.

Microsoft has provided a workaround that involves removing support for this ActiveX Control within Internet Explorer using all of the Class Identifiers listed in the workaround section of the following link <http://www.microsoft.com/technet/security/advisory/972890.mspx> Alternatively, an automatic workaround solution can be found in Microsoft Knowledge Base Article 972890 (<http://support.microsoft.com/kb/972890>)

How is this vulnerability being exploited?

In a Web-based attack scenario, an attacker could compromise a legitimate web site (web sites that accept or host user-provided content or advertisements are prime targets for compromise) and link to servers under their control that exploits this vulnerability install malware on the victims system. Alternatively, an attacker could attempt to lure victims directly to their malicious web sites via links in email messages in order to exploit the vulnerability.

How does IDF shield this vulnerability from attack?

Trend Micro™ has released three new security rules that shield this vulnerability from attack:

- **Rule 1003606:** Microsoft Windows 'MPEG2TuneRequest' Object Remote Code Execution
 - Exploit facing rule that protects against published exploits of the Microsoft Windows MPEG2TuneRequest ActiveX Control Object vulnerability
- **Rule 1003605:** Microsoft Windows 'MPEG2TuneRequest' Object Remote Code Execution Vulnerability
 - Smart rule designed to shield the specific Class Identifier currently being used in published exploits and to protect against all future variations of attacks against this Class Identifier
- **Rule 1003609:** Com Object Instantiation Memory Corruption – July 2009
 - Smart rule designed to shield all vulnerable Class Identifiers from attack as further protection against new attack variants of the Microsoft Windows MPEG2TuneRequest ActiveX Control Object vulnerability

- **Rule 1002061:** Identified Suspicious JavaScript Encoded Shellcode
 - Smart rule designed to detect malicious JavaScript encoded shellcode and in this case was successful in detecting the malicious payloads in the known exploits of the Microsoft Windows MPEG2TuneRequest ActiveX Control Object vulnerability

Which Microsoft Operating Systems are affected?

- Microsoft Windows XP 0
- Microsoft Windows XP 64-bit Edition
- Microsoft Windows XP 64-bit Edition SP1
- Microsoft Windows XP 64-bit Edition Version 2003
- Microsoft Windows XP 64-bit Edition Version 2003 SP1
- Microsoft Windows XP Gold 0
- Microsoft Windows XP Home
- Microsoft Windows XP Home SP1
- Microsoft Windows XP Home SP2
- Microsoft Windows XP Home SP3
- Microsoft Windows XP Media Center Edition
- Microsoft Windows XP Media Center Edition SP1
- Microsoft Windows XP Media Center Edition SP2
- Microsoft Windows XP Media Center Edition SP3
- Microsoft Windows XP Professional
- Microsoft Windows XP Professional SP1
- Microsoft Windows XP Professional SP2
- Microsoft Windows XP Professional SP3
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows XP Professional x64 Edition SP2
- Microsoft Windows XP Professional x64 Edition SP3
- Microsoft Windows XP Tablet PC Edition
- Microsoft Windows XP Tablet PC Edition SP1
- Microsoft Windows XP Tablet PC Edition SP2
- Microsoft Windows XP Tablet PC Edition SP3

- Microsoft Windows Server 2003 Service Pack 2
- Microsoft Windows 2003 x64 Edition Service Pack 2
- Windows Server 2003 with SP2 for Itanium-based systems

Additional reference Links:

- <http://www.microsoft.com/technet/security/advisory/972890.mspx>
- <http://support.microsoft.com/kb/972890>
- <http://isc.sans.org/diary.html?storyid=6733&rss>
- <http://www.csis.dk/en/news/news.asp?tekstID=799>
- http://www.theregister.co.uk/2009/07/06/new_microsoft_exploit_in_wild/

Frequently Asked Questions

[What is a zero-day vulnerability?](#)

[Why are multiple IDF rules required to shield this vulnerability?](#)

[What is an emergency security update?](#)

[How did we create these new rules?](#)

[Did any of our security rules offer protection in advance of the release of these three rules?](#)

[Are there any situations where IDF would not detect attacks against this vulnerability?](#)

[Are there known exploits of this vulnerability already?](#)

What is a zero-day vulnerability?

A zero-day vulnerability is a vulnerability which is unknown or undisclosed to the vendor, or for which no security fix is currently available. [\(Back\)](#)

Why are multiple IDF rules required to shield this vulnerability?

IDF provides multiple rules to provide comprehensive protection with each rule having a specific role in detecting and shielding attacks against the Microsoft Windows MPEG2TuneRequest ActiveX Control Object vulnerability. [\(Back\)](#)

- Rule 1002061 provides generic protection against JavaScript encoded shellcode attacks
- Rule 1003606 provides protection against known exploits
- Rule 1003605 shields the Class Identifier used in known exploits from all attack variations
- Rule 1003609 shields all vulnerable Class Identifiers from all attack variations

What is an emergency security update?

IDF Security updates are normally released every two weeks (2nd and 4th Tuesday of every month). For critical vulnerabilities that can affect our customers, we will provide an emergency update in advance of

our regularly scheduled security update. Emergency security updates will only contain the security rules necessary to shield the critical vulnerabilities. [\(Back\)](#)

How did we create these new rules?

Over 100 sources of public, private and government data are systematically and continuously monitored to identify and correlate new relevant threats and vulnerabilities. In addition, we are part of the Microsoft Active Protections Program and receive vulnerability information from the Microsoft Security Response Center. All of this vulnerability information is used to assist with the research and development of security rules used in the IDF product. [\(Back\)](#)

Did any of our security rules offer protection in advance of the release of these three rules?

Yes, an existing IDF rule (*1002061: Identified Suspicious JavaScript Encoded Shellcode*) would have also protected against currently known exploits of this vulnerability. [\(Back\)](#)

Are there any situations where IDF would not detect attacks against this vulnerability?

Yes, the IDF rules for this vulnerability would not be able to detect and protect attacks against this vulnerability under the following situations:

- The attack is sent over a HTTPS connection
- The attack uses evasive techniques (JavaScript Encoding) to obfuscate the Class Identifier [\(Back\)](#)

Are there known exploits of this vulnerability already?

Yes, a number of web sites are reporting exploits of this vulnerability, links to recent news articles is provided below. [\(Back\)](#)

- http://www.theregister.co.uk/2009/07/06/new_microsoft_exploit_in_wild/
- <http://www.securityfocus.com/brief/984>